Information-disturbance tradeoff in estimating a maximally entangled state

Massimiliano F. Sacchi
QUIT Quantum Information Theory Group and*
CNR - Istituto Nazionale per la Fisica della Materia,
Dipartimento di Fisica "A. Volta", via A. Bassi 6, I-27100 Pavia, Italy†
(Dated: February 1, 2008)

We derive the amount of information retrieved by a quantum measurement in estimating an unknown maximally entangled state, along with the pertaining disturbance on the state itself. The optimal tradeoff between information and disturbance is obtained, and a corresponding optimal measurement is provided.

PACS numbers:

The tradeoff between information retrieved from a quantum measurement and the disturbance caused on the state of a quantum system is a fundamental concept of quantum mechanics and has received a lot of attention in the literature [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]. Such an issue is studied for both foundations and its enormous relevance in practice, in the realm of quantum key distribution and quantum cryptography [17, 18].

A part from many heuristic statements of the information-disturbance tradeoff, just a few quantitative derivations have been obtained in the scenario of quantum state estimation [19, 20]. The optimal tradeoff has been derived in the following cases: in estimating a single copy of an unknown pure state [7], many copies of identically prepared pure qubits [9], a single copy of a pure state generated by independent phase-shifts [13], and an unknown coherent state [16]. Recently, experiment realization of minimal disturbance measurements has been also reported [14, 16].

The problem is typically the following. One performs a measurement on a quantum state picked (randomly, or according to an assigned a priori distribution) from a known set, and evaluates the retrieved information along with the disturbance caused on the state. The physical transformation will be described by a quantum operation (in an old-fashioned terminology, a measurement of the first kind, where it is possible to describe the state *after* the measurement). To quantify the tradeoff between information and disturbance, one can adopt two mean fidelities [7]: the estimation fidelity G, which evaluates on average the best guess we can do of the original state on the basis of the measurement outcome, and the operation fidelity F, which measures the average resemblance of the state of the system after the measurement to the original one.

In this Letter, we study and provide the optimal tradeoff between estimation and operation fidelities when the state is a completely unknown maximally entangled state of finite-dimensional quantum systems. We also provide a measurement that achieves such an optimal tradeoff.

The interest in maximally entangled states lies in the fact that they represent a major resource in quantum information technology, e.g. in quantum teleportation [21] and quantum cryptography [18]. The study of the information-disturbance tradeoff for maximally entangled states can become of practical relevance for posing general limits in information eavesdropping and for analyzing security of quantum cryptographic communications.

Our results will be obtained by exploiting the group symmetry of the problem, which allows us to restrict our analysis on *covariant measurement instruments*. In fact, the property of covariance generally leads to a striking simplification of problems that may look intractable, and has been thoroughly used in the context of state and parameter estimation [19, 20].

A measurement process on a quantum state ρ with outcomes $\{r\}$ is described by an *instrument* [22], namely a set of trace-decreasing completely positive (CP) maps $\{\mathcal{E}_r\}$. Each map can then be written in the Kraus form [23]

$$\mathcal{E}_r(\rho) = \sum_\mu A_{r\mu} \rho A^\dagger_{r\mu} \,, \tag{1}$$

and provides the state after the measurement

$$\rho_r = \frac{\mathcal{E}_r(\rho)}{\mathrm{Tr}[\mathcal{E}_r(\rho)]} \,, \tag{2}$$

along with the probability of outcome

$$p_r = \mathrm{Tr}[\mathcal{E}_r(\rho)] = \mathrm{Tr}\left[\sum_\mu A^\dagger_{r\mu} A_{r\mu} \rho\right] \,. \tag{3}$$

The set of positive operators $\{\Pi_r = \sum_\mu A^\dagger_{r\mu} A_{r\mu}\}$ is known as positive operator-valued measure (POVM), and normalization requires the completeness relation $\sum_r \Pi_r = I$. This is equivalent to require that the map $\sum_r \mathcal{E}_r$ is trace-preserving.

When considering bipartite systems it is convenient to exploit the natural isomorphism between operators A on the Hilbert space $\mathcal{H}$ and vectors $|A\rangle\!\rangle$ in $\mathcal{H}^{\otimes 2}$, defined through the equation

$$|A\rangle\!\rangle \equiv \sum_{m,n} \langle m|A|n\rangle |m\rangle |n\rangle \,. \tag{4}$$

We will make repeated use of the following identities [24]

$$A \otimes B | C\rangle\!\rangle = | ACB^\tau\rangle\!\rangle \,, \quad (5)$$
$$\mathrm{Tr}_1[| A\rangle\!\rangle\langle\!\langle B |] = A^\tau B^* \,, \quad (6)$$
$$\mathrm{Tr}_2[| A\rangle\!\rangle\langle\!\langle B |] = AB^\dagger \,, \quad (7)$$
$$\langle\!\langle A | B\rangle\!\rangle = \mathrm{Tr}[A^\dagger B] \,, \quad (8)$$

where τ and $*$ denote transposition and complex conjugation with respect to the fixed basis in Eq. (4), and Tr_i represents the partial trace over the ith Hilbert space. A maximally entangled state in $\mathcal{H} \otimes \mathcal{H}$, with $\dim(\mathcal{H}) = d$ will then be written as $\frac{1}{\sqrt{d}} | U_g\rangle\!\rangle$, where U_g is a unitary $d \times d$ matrix, i.e. g denotes an element of the group $SU(d)$. When performing averages on group parameters, for convenience we will take the normalized invariant Haar measure dg over the group, i.e. $\int_{SU(d)} dg = 1$, and we will also omit $SU(d)$ from the symbol of integral. To avoid confusion when the number of Hilbert spaces proliferates, we will also used the notation $| A\rangle\!\rangle_{ij}$ when it is necessary to identify the vector in the Hilbert space $\mathcal{H}_i \otimes \mathcal{H}_j$. Similarly, $A^{(ij)}$ will denote a linear operator acting on $\mathcal{H}_i \otimes \mathcal{H}_j$.

The operation fidelity F evaluates on average how much the state after the measurement resembles the original one, in terms of the squared modulus of the scalar product. Hence, for a measurement of an unknown maximally entangled state, one has

$$F = \frac{1}{d^2} \int dg \sum_{r\mu} |\langle\!\langle U_g | A_{r\mu} | U_g\rangle\!\rangle|^2 \,, \quad (9)$$

where $\{A_{r\mu}\}$ are the Kraus operators of the measurement instrument (1). For each measurement outcome r, one guesses a maximally entangled state $\frac{1}{\sqrt{d}} | U_r\rangle\!\rangle$ and the corresponding average estimation fidelity is given by

$$G = \frac{1}{d^3} \int dg \sum_{r\mu} \langle\!\langle U_g | A^\dagger_{r\mu} A_{r\mu} | U_g\rangle\!\rangle \, |\langle\!\langle U_r | U_g\rangle\!\rangle|^2 \,. \quad (10)$$

Without loss of generality, we can restrict out attention to *covariant* instruments, that satisfy

$$\mathcal{E}_h(U_g \otimes I \, \rho \, U_g^\dagger \otimes I) = (U_g \otimes I) \mathcal{E}_{g^{-1}h}(\rho)(U_g^\dagger \otimes I) \,. \quad (11)$$

In fact, for any instrument (1) and guess $\frac{1}{\sqrt{d}} | U_r\rangle\!\rangle$ in (10), one can easily show that the covariant instrument

$$\begin{aligned} \mathcal{E}_h(\rho) \;&=\; \sum_{r\mu} (U_h U_r^\dagger \otimes I) A_{r\mu} (U_r U_h^\dagger \otimes I) \, \rho \\ &\times \; (U_h U_r^\dagger \otimes I) A^\dagger_{r\mu} (U_r U_h^\dagger \otimes I) \,, \end{aligned} \quad (12)$$

with continuous outcome $h \in SU(d)$, along with the guess $\frac{1}{\sqrt{d}} | U_h\rangle\!\rangle$, provides the same values of F and G as the original instrument (1).

It is useful now to consider the Jamiołkowski representation [26], that gives a one-to-one correspondence between a CP map $\mathcal{E}$ from $\mathcal{H}_{in}$ to $\mathcal{H}_{out}$ and a positive operator R on $\mathcal{H}_{out} \otimes \mathcal{H}_{in}$ through the equations

$$\begin{aligned} &\mathcal{E}(\rho) = \mathrm{Tr}_{in}[(I_{out} \otimes \rho^\tau) R] \,, \\ &R = (\mathcal{E} \otimes I_{in}) | I\rangle\!\rangle\langle\!\langle I | \,. \end{aligned} \quad (13)$$

When $\mathcal{E}$ is trace preserving, one has also $\mathrm{Tr}_{out}[R] = I_{in}$.

For covariant instruments $\mathcal{E}_g$ acting on $\mathcal{H}_1 \otimes \mathcal{H}_2$ as in Eq. (12), the operator R_g acts on $\mathcal{H}^{\otimes 4}$, and has the form

$$R_g = U_g^{(1)} \otimes U_g^{*(3)} R_0 U_g^{\dagger(1)} \otimes U_g^{\tau(3)} \,, \quad (14)$$

with $R_0 \geq 0$, and the trace-preserving condition

$$\int dg \, \mathrm{Tr}_{34}[R_g] = I^{(12)} \,. \quad (15)$$

From Eq. (14) and the identity (Schur's lemma for irreducible group representations [25])

$$\int dg \, U_g X U_g^\dagger = \frac{1}{d} \mathrm{Tr}[X] I \,, \quad (16)$$

it follows that condition (15) is equivalent to

$$\mathrm{Tr}_{1,3,4}[R_0] = d I^{(2)} \,, \quad (17)$$

which implies $\mathrm{Tr}[R_0] = d^2$.

By defining the projector on the unnormalized maximally entangled vector of $\mathcal{H}_i \otimes \mathcal{H}_j$ as

$$\mathcal{I}^{(ij)} = | I\rangle\!\rangle_{ij\,ij}\langle\!\langle I | \,, \quad (18)$$

the fidelities F and G can be written as $F = \mathrm{Tr}[R_F R_0]$ and $G = \mathrm{Tr}[R_G R_0]$, where R_F and R_G are the following positive operators

$$\begin{aligned} R_F \;&=\; \frac{1}{d^2} \int dg \, U_g^{(1)} \otimes U_g^{*(3)} \, \mathcal{I}^{(12)} \otimes \mathcal{I}^{(34)} \, U_g^{\dagger(1)} \otimes U_g^{\tau(3)} \,, \\ R_G \;&=\; \frac{1}{d^3} \int dg \, |\langle\!\langle I | U_g\rangle\!\rangle|^2 \, U_g^{*(3)} (I^{(12)} \otimes \mathcal{I}^{(34)}) U_g^{\tau(3)} \\ &=\; \frac{1}{d} \{ I^{(12)} \otimes \mathrm{Tr}_{12}[\mathcal{I}^{(12)} \otimes I^{(34)} R_F] \} \,. \end{aligned}$$

Using the identity (Schur's lemma for reducible group representations [25])

$$\begin{aligned} &\int dg \, U_g \otimes U_g^* \, Y \, U_g^\dagger \otimes U_g^\tau = \mathrm{Tr}[Y \mathcal{I}/d] \mathcal{I}/d \\ &+ \mathrm{Tr}[Y(I - \mathcal{I}/d)] \frac{I - \mathcal{I}/d}{d^2 - 1} \,, \end{aligned} \quad (19)$$

one obtains

$$\begin{aligned} R_F \;&=\; \frac{1}{d^2(d^2-1)} \Big[I + \mathcal{I}^{(13)} \otimes \mathcal{I}^{(24)} \\ &-\; \frac{1}{d} (I^{(13)} \otimes \mathcal{I}^{(24)} + \mathcal{I}^{(13)} \otimes I^{(24)}) \Big] \,, \\ R_G \;&=\; \frac{1}{d^2(d^2-1)} \left[\left(1 - \frac{2}{d^2} \right) I + \frac{1}{d} I^{(12)} \otimes \mathcal{I}^{(34)} \right] \,. \end{aligned}$$

The optimal tradeoff between F and G can be found by looking for a positive operator R_0 that satisfies the trace-preserving condition (17) and maximizes a convex combination

$$pG + (1-p)F = \mathrm{Tr}\{[pR_G + (1-p)R_F]R_0\}\ , \qquad (20)$$

where $p \in [0,1]$ controls the tradeoff between the quality of the state estimation and the quality of the output replica of the state. Then, R_0 will provide a covariant instrument that achieves the optimal tradeoff. It turns out that for any p the eigenvector corresponding to the maximum eigenvalue of $C(p) \equiv pR_G + (1-p)R_F$ is of the form [27]

$$|\chi\rangle = x|\, I\rangle\rangle_{12}|\, I\rangle\rangle_{34} + y|\, I\rangle\rangle_{13}|\, I\rangle\rangle_{24}\ , \qquad (21)$$

with suitable positive x and y. Upon taking R_0 proportional to $|\chi\rangle\langle\chi|$, the covariant instrument will then be optimal. In fact, condition (17) can be easily verified, and the normalization can be derived from the condition $\mathrm{Tr}[R_0] = d^2$.

From Eqs. (13) and (14), it follows that the optimal tradeoff can be reached by an instrument with Kraus operators

$$A_g = a|\, U_g\rangle\rangle\langle\langle U_g\,| + bI\ , \qquad (22)$$

where $0 \le a \le 1$, and $b = \frac{1}{d}(\sqrt{d^2(1-a^2)+a^2} - a)$. In fact, condition $\mathrm{Tr}[R_0] = d^2$ is equivalent to $(a^2+b^2)d^2 + 2abd = d^2$. The corresponding fidelities are given by

$$\begin{aligned} F &= \frac{1}{d^2(d^2-1)}[d^2 + (d^2-2)(a+bd)^2] = 1 - \frac{d^2-2}{d^2}a^2\ , \\ G &= \frac{1}{d^2(d^2-1)}[d^2 - 2 + (ad+b)^2] = \frac{2-b^2}{d^2}\ . \end{aligned}$$

Notice that the instrument given by operators (22) is *pure*, in the sense that it leaves pure states as pure. When no measurement is performed ($a = 0$), one has $F = 1$ and $G = \frac{1}{d^2}$, which is equivalent to randomly guessing the unknown state. The optimal estimation can be obtained by a Bell measurement ($b = 0$), namely by projectors on maximally entangled states, and gives $F = G = \frac{2}{d^2}$.

Upon eliminating a and b, we obtain the optimal tradeoff between F and G

$$\sqrt{(d^2-2)(2-d^2G)} = \sqrt{(d^2-1)F-1} - \sqrt{1-F}\ , \qquad (23)$$

or, equivalently,

$$\begin{aligned} &\sqrt{\frac{d^2}{d^2-2}\left(F - \frac{1}{d^2-1}\right)} \qquad (24) \\ &= \sqrt{G - \frac{d^2-2}{d^2(d^2-1)}} + \sqrt{(d^2-1)\left(\frac{2}{d^2} - G\right)}\ . \end{aligned}$$

Such an optimal tradeoff overcomes the corresponding one for a completely unknown state [7] in a Hilbert space with dimension d^2, i.e. for a fixed value of the estimation fidelity G one can achieve here a better value of the operation fidelity F. In other words, when a partial knowledge of the set of states is available (here, the fact that the states are maximally entangled), one can obtain the same estimation fidelity with a smaller disturbance of the state.

We can introduce two normalized quantities—a sort of visibilities—that can be interpreted as the average information I retrieved from the quantum measurement and the average disturbance D affecting the original quantum state as follows:

$$I = \frac{G - G_0}{G_{max} - G_0} = d^2G - 1 = 1 - b^2\ , \qquad (25)$$

where $G_0 = \frac{1}{d^2}$ is the value of G for random guess and $G_{max} = \frac{2}{d^2}$ is the maximum value attainable by G;

$$D = \frac{1-F}{1-F_{min}} = \frac{d^2(1-F)}{d^2-2} = a^2\ , \qquad (26)$$

where $F_{min} = \frac{2}{d^2}$ represents the average fidelity with the maximally chaotic state $\frac{I}{d^2}$. Clearly, one has $0 \le I \le 1$, and $0 \le D \le 1$. In this way, after some algebra one obtains the quadratic expression

$$d^2(D-I)^2 - 4D(1-I) = 0 \qquad (27)$$

that gives the optimal information-disturbance tradeoff. We plot in Fig. 1 the behavior of the tradeoff for dimension $d = 2, 4$, and 8. For a given value of the information I, the curves $D(I)$ represent a lower bound for the disturbance of any measurement instrument.

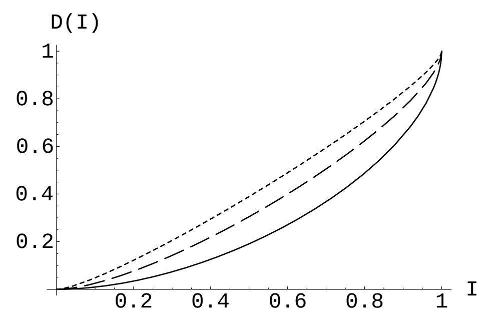

FIG. 1: Optimal information-disturbance tradeoff in estimating an unknown maximally entangled state for dimension $d = 2$ (solid line), $d = 4$ (dashed line), and $d = 8$ (dotted), where I and D are defined through Eqs. (25) and (26) in terms of the estimation and operation fidelities G and F, respectively. For given value of the retrieved information I, the curves $D(I)$ are a lower bound for the disturbance of any measurement instrument.

The optimal tradeoff is reached by a measuring instrument (22) whose Kraus operator are a coherent superpositions of two extreme measurements: the identity map

and the optimal map for estimating an unknown maximally entangled state. It can be easily shown that the discrete version $\{\mathcal{E}_r\}$ of such an instrument with Kraus operators

$$A_r = \frac{1}{d}(a|\, U_r\rangle\rangle\langle\langle U_r\,| + bI)\ , \qquad r = 1, 2, ..., d^2\ , \quad (28)$$

and orthogonal $\{|\, U_r\rangle\rangle\}$, namely $\langle\langle U_r\,|U_s\rangle\rangle = d\delta_{rs}$, achieves the same values of F and G, and hence the optimal tradeoff as well. Notice that the POVM $A_r^\dagger A_r$ corresponding to this instrument is made of projectors on so-called Werner states [29], i.e. convex mixtures of maximally entangled and maximally chaotic states. The experimental realization of such a kind of measurement could be investigated for hyperentangled two-photon states, for which Bell measurements have been already demonstrated [30].

In conclusion, a tight bound between the quality of estimation of an unknown maximally entangled state and the degree the initial state has to be changed by this operation has been derived. Such a bound can be achieved by noisy Bell measurements, where the noise continuously controls the tradeoff between the information retrieved by the measurement and the disturbance on the original state.

Acknowledgments. This work has been sponsored by Ministero Italiano dell'Università e della Ricerca (MIUR) through FIRB (2001) and PRIN 2005.

* URL: `http://www.qubit.it`
† Also at CNISM - Consorzio Nazionale Interuniversitario per le Scienze Fisiche della Materia

[1] W. Heisenberg, Zeitsch. Phys. **43**, 172 (1927).
[2] K. Wódkiewicz, Phys. Lett. A **124**, 207 (1987).
[3] M. O. Scully, B.-G. Englert, and H. Walther, Nature **351**, 111 (1991).
[4] S. Stenholm, Ann. Phys. **218**, 233 (1992).
[5] B.-G. Englert, Phys. Rev. Lett. **77**, 2154 (1996).
[6] C. A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).
[7] K. Banaszek, Phys. Rev. Lett. **86**, 1366 (2001).
[8] C. A. Fuchs and K. Jacobs, Phys. Rev. A **63**, 062305 (2001).
[9] K. Banaszek and I. Devetak, Phys. Rev. A **64**, 052307 (2001).
[10] H. Barnum, quant-ph/0205155.
[11] G. M. D'Ariano, Fortschr. Phys. **51**, 318 (2003).
[12] M. Ozawa, Ann. Phys. **311**, 350 (2004).
[13] L. Mišta Jr., J. Fiurášek, and R. Filip, Phys. Rev. A **72**, 012311 (2005).
[14] F. Sciarrino, M. Ricci, F. De Martini, R. Filip, and L. Mišta Jr., Phys. Rev. Lett. **96**, 020408 (2006).
[15] L. Maccone, Phys. Rev. A **73**, 042307 (2006).
[16] U. L. Andersen, M. Sabuncu, R. Filip, and G. Leuchs, Phys. Rev. Lett. **96**, 020409 (2006).
[17] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175; C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[18] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); Nature **358**, 14 (1992).
[19] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North Holland, Amsterdam, 1982).
[20] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995); R. Derka, V. Buzek, and A. K. Ekert, Phys. Rev. Lett. **80**, 1571 (1998); J. I. Latorre, P. Pascual, and R. Tarrach, Phys. Rev. Lett. **81**, 1351 (1998); G. Vidal, J. I. Latorre, P. Pascual, and R. Tarrach, Phys. Rev. A **60**, 126 (1999); A. Acín, J. I. Latorre, and P. Pascual, Phys. Rev. A **61**, 022113 (2000); G. Chiribella, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, Phys. Rev. A **70**, 062105 (2004); G. Chiribella, G. M. D'Ariano, and M. F. Sacchi, Phys. Rev. A **72**, 042338 (2005).
[21] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[22] E. B. Davies and J. T Lewis, Commun. Math. Phys. **17**, 239 (1970); M. Ozawa, J. Math. Phys. **25**, 79 (1984).
[23] K. Kraus, *States, Effects, and Operations*, (Springer-Verlag, Berlin, 1983).
[24] G. M. D'Ariano, P. Lo Presti, and M. F. Sacchi, Phys. Lett. A **272**, 32 (2000).
[25] D. P. Zhelobenko, *Compact Lie Groups and Their Representations* (American Mathematical Society, Providence, RI, 1973).
[26] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972); M. F. Sacchi, Phys. Rev. A **63**, 054104 (2001).
[27] It can be shown analytically that the operator norm of $C(p)$ (i.e. its maximum eigenvalue) satisfies

$$\|C(p)\| = \frac{1}{2d^4(d^2-1)}\{d^4 - 4p + 3d^2p - d^4p$$
$$+ d\sqrt{d^2[2-d^2(1-p)-p]^2 + 4(d^2-2)p(1-p)}\}$$

for $d = 2, 3$, and the corresponding eigenvector is of the form as in Eq. (21), with $x = 1$ and

$$y = \frac{1}{2p}\{d^3(1-p) - d(2-p) +$$
$$\sqrt{d^2[2-d^2(1-p)-p]^2 + 4(d^2-2)p(1-p)}\}$$

For higher values of d, such a result can be checked, for example, by means of the power method [28].
[28] E. Isaacson and H. B Keller, *Analysis of numerical methods* (Dover, N. Y., 1994).
[29] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[30] S. P. Walborn, S. Pádua, and C. H. Monken, Phys. Rev. A **68**, 042313 (2003).